EECS 565: Introduction to Information and Computer Security

5 September 2025

Message Decryption

1. "MSOKKJCOSXOEEKDTOSLGFWCMCHSUSGX"
key length = 2; firstWordLength = 6

CAESARSWIFEMUSTBEABOVESUSPICION | KS

Elapsed time: 0.620 seconds

2.
"PSPDYLOAFSGFREQKKPOERNIYVSDZSUOVGXSRRIPWERDIPCFSDIQZIASEJVCGXAYBGYXFPSREK
FMEX
EBIYDGFKREOWGXEQSXSKXGYRRRVMEKFFIPIWJSKFDJMBGCC"
keyLength=3; firstWordLength = 7

FORTUNEWHICHHASAGREATDEALOFPOWERINOTHERMATTERSBUTESPECIALLYINWARCANBRINGABOUTGREATCHANGESINASITUATIONTHROUGHVERYSLIGHTFORCES | KEY

Elapsed time: 34.620 seconds

3. "MTZHZEOQKASVBDOWMWMKMNYIIHVWPEXJA"
keyLength=4; firstWordLength = 10

EXPERIENCEISTHETEACHEROFALLTHINGS | IWKD

Elapsed time: 375.313 seconds

4. "SQLIMXEEKSXMDOSBITOTYVECRDXSCRURZYPOHRG"
keyLength=5; firstWordLength = 11

IMAGINATIONISMOREIMPORTANTTHANKNOWLEDGE | KELCE

Elapsed time: 34807.514 seconds

5. "LDWMEKPOPSWNOAVBIDHIPCEWAETYRVOAUPSINOVDIEDHCDSELHCCPVHRPOHZUSERSFS"
keyLength=6; firstWordLength = 9

EDUCATIONISWHATREMAINSAFTERONEHASFORGOTTENWHATONEHASLEARNEDINSCHOOL | HACKER

Elapsed time: 97200.211 seconds

6. "VVVLZWWPBWHZDKBTXLDCGOTGTGRWAQWZSDHEMXLBELUMO"
keyLength=7; firstWordLength = 13

(Did not decipher this message)

Elapsed time: INVALID

Discussion Questions

(1) discuss the efficiency of password cracking;

Password cracking is efficient with shift ciphers but not with Vigenère ciphers. Shift ciphers will only have 25 options to check from, which can be done in seconds. Vigenère ciphers uses a word to encrypt the message, which if the hacker has no information about the key or the first word, trying to decrypt the message will be very time consuming. Even with the first word, key length and small optimizations, checking all possibilities for keys with more than 5 letters will take a long time. That is why I believe password cracking for a Vigenère cipher is inefficient.

(2) discuss the optimization technique(s) that you use and how it can improve cracking efficiency.

I filtered out the first word list to only check the words that are equal to the first word length. I believe the time complexity was reduced as the program did not have to check every word in the first word list.